NEW CRITICAL VULNERABILITY ADVISORY: CVE-2026-67289

Summary

CVE-2026-67289 is a newly disclosed Critical vulnerability. It is not yet on CISA's actively-exploited list; treat it as proactive patching before it is weaponised. FreeRDP before 3.29.0 (affected versions <= 3.28.0) does not validate CRLF and control characters in the server-controlled RDP redirection TargetNetAddress field. This value is copied into the client's ServerHostname and, when the client connects through an HTTP proxy, is written directly into the proxy CONNECT request line and Host header by http_proxy_connect() without filtering. A malicious or compromised RDP server can send a crafted redirection PDU containing embedded control characters to inject arbitrary headers/requests into the HTTP proxy CONNECT request.

What we know

- **CVE:** CVE-2026-67289
- **Status:** Newly disclosed, not yet known-exploited (not on CISA KEV)
- **Severity:** CVSS 9.8 Critical, Network-exploitable, no privileges required, no user interaction (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
- **Exploitation likelihood (EPSS):** 0%

Recommended action

Patch as a fix becomes available, prioritised by the exposure and EPSS above. Until then, restrict network access to the affected service now (segment it, put it behind a VPN, or take it offline) until you can patch. This does not yet trigger CRA 24-hour reporting, which requires active exploitation, but patching ahead of exploitation is the whole point.

Sources: NIST NVD. Public data; an advisory of a newly disclosed vulnerability, not an incident report. Verify applicability to your estate before acting.